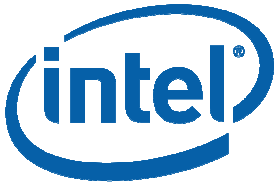
Open Source Technology Center

Trusted Boot: Verifying the Xen Launch

Joseph Cihula

Intel Corp.



Fall 2007 Xen Summit

Agenda

- Intel® Trusted Execution Technology Overview
- What is Trusted Boot (tboot)?
- Why use Trusted Boot?
- Configuring Your System
- Creating and Provisioning Policies
- Tboot Support in Xen

Intel® Trusted Execution Technology (Intel® TXT)

Formerly called LT (LaGrande Technology)

Removes BIOS/bootloader/OS/etc. from trust chain

- Creates dynamic root of trust (DRTM)

HW-based measured and verified launch

- Does not require Intel® Virtualization Technology (Intel® VT)

Platform configuration protection

Reset memory protection

Safer Mode Extensions (SMX)

- Intel TXT processor instructions

Spec available:
http://www.intel.com/technology/security/

What is Trusted Boot (tboot)?

Open source, pre-kernel/VMM module

Uses Intel TXT to perform verified launch of OS kernel/VMM

- Today only supports Xen

Available from http://sourceforge.net/projects/tboot

- Mercurial repo at http://tboot.sourceforge.net/hg/tboot.hg
- Also tarballs of the source

Project also contains tools for policy creation and provisioning

- Intel TXT Launch Control Policy (LCP)
- Tboot Verified Launch policy

Why Use Trusted Boot?

Trusted Boot provides a foundation for a Trusted Xen

- Root of trust is in hardware: Intel TXT dynamic launch
- Tboot is verified by Intel TXT Launch Control Policy (LCP)
  - Part of measured launch
  - Can optionally verify BIOS
- Tboot Verified Launch verifies Xen and Dom0 (+ initrd)
  - Dom0 trust could be extended via IMA, disaggregation, etc.

Drop-in to Xen 3.2

- No changes to GRUB

  (Should be easily extensible to other bootloaders)
- No-op on non-TXT systems

intel
Open Source Technology Center

Configuring Your System

Xen 3.2 supports tboot

As of c/s 16267:26fb702fd8cf

1. Get tboot source and build

- Optional top-level Makefile targets: {build, install, clean}-tboot
  - Will download tboot.tar.gz from SourceForge

2. Get SINIT AC Module (`BRLK_SINIT_20070910_release.BIN`)

- From OEM or Trusted Boot SourceForge site (soon)

3. Edit grub.conf

```
title Xen 3.2 w/ Intel(R) Trusted Execution Technology
   root (hd0,1)
   kernel /tboot.gz
   module /xen.gz no-real-mode dom0_mem=524288 com1=115200,8n1
   module /vmlinuz-2.6.18-xen root=/dev/hda1 ro
   module /initrd-2.6.18-xen.img
   module /BRLK_SINIT_20070910_release.BIN
```

4. Boot

- Monitor the serial output for tboot progress

intel
Open Source Technology Center

Policies

Intel TXT LCP:

- Two types of policies: SRTM (BIOS) and MLE (tboot)
  - SRTM policy is optional; based on PCRs
- MLE policy is (list of) SHA-1 hash(es)
  - Optional SINIT revocation version
- Policy stored in TPM NV
  - Multiple hashes require separate file (whose hash is in TPM NV)

Tboot Verified Launch policy:

- Currently two components verified: hypervisor and Dom0
  - Will generalize in future
- Policies are (list of) SHA-1 hash(es) and policy type
  - Policy type determines behavior when errors are encountered:
    - Continue for all non-fatal errors
    - Halt except for verification failures
    - Halt for all errors
- Policies stored in TPM NV

intel
Open Source Technology Center

Preparing the TPM

Only need to do these once

Take ownership of the TPM:

1. `modprobe tpm_tis`
2. `tcsd`
3. `tpm_takeownership`
   - Choose password for TPM (ownerauth) and for SRK, confirming each

Define tboot error TPM NV index:

1. `lcptools/tpmnv_defindex -i 0x20000002 -s 8 -pv 0 -rl 0x07 -wl 0x07 -p <ownerauth>`

Define policy TPM NV indices:

1. `lcptools/tpmnv_defindex -i owner -p <ownerauth>`
2. `lcptools/tpmnv_defindex -i 0x20000001 -s 512 -pv 0x02 -p <ownerauth>`

intel
Open Source Technology Center

Creating Policies

Create LCP policy:

1. `lcptools/lcp_mlehash /boot/tboot.gz > mle_hash`
2. `lcptools/lcp_crtpol -t hashonly -m mle_hash -o lcp.pol`

Create Verified Launch policy:

1. `tb_polgen/tb_polgen –-create --policy_type nonfatal --uuid vmm --hash_type hash --file tcb.pol --cmdline “/xen.gz no-real-mode dom0_mem=524288 com1=115200,8n1” /boot/xen.gz`
2. `tb_polgen/tb_polgen --create --uuid dom0 --hash_type hash --file tcb.pol --cmdline “/vmlinuz-2.6.18-xen root=/dev/hda1 ro” /boot/vmlinuz-2.6.18-xen /boot/initrd-2.6.18-xen.img`

Open Source Technology Center

Provisioning Policies

Write LCP and Verified Launch policies to TPM:

```
(modprobe tpm_tis; tcsd;)
1. lcptools/lcp_writepol -i owner -f lcp.pol
   -p <ownerauth>
2. lcptools/lcp_writepol -i 0x20000001
   -f tcb.pol -p <ownerauth>
```


intel
Open Source Technology Center

Tboot Support in Xen

"Discovery" of tboot shared page

- Passed as '`tboot=0x<phys_addr>`' command line option
- Contains tboot log addr, Sx data and trampoline/return addrs

Support E820_UNUSABLE memory type as reserving memory from Dom0

- Used by tboot to restrict Dom0 access to TXT data areas
- Eventually to protect tboot

Sx return into tboot for shutdown

- S3/4/5 w/o GETSEC[SEXIT] will hang/reboot system, so must call back into tboot to cleanup and shutdown

intel
Open Source Technology Center

Legal Content

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY RELATING TO SALE AND/OR USE OF INTEL PRODUCTS, INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT, OR OTHER INTELLECTUAL PROPERTY RIGHT.

Intel may make changes to specifications, product descriptions, and plans at any time, without notice.

All dates provided are subject to change without notice.

Intel is a trademark of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2007, Intel Corporation. All rights are protected.

Open Source Technology Center